Office of Audits
Office of Inspector General
U.S. General Services Administration

# Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2020

November 18, 2020

**SENSITIVE INFORMATION REMOVED FOR PUBLIC RELEASE**

December 4, 2020

MEMORANDUM FOR: EMILY W. MURPHY
ADMINISTRATOR (A)

FROM: CAROL F. OCHOA
INSPECTOR GENERAL (J)

SUBJECT: Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2020, dated November 18, 2020

As required by the *Federal Information Security Modernization Act of 2014* (FISMA), attached is the annual independent evaluation report on the effectiveness of GSA's Information Security Program and Practices for Fiscal Year 2020. This restricted report contains specific systems' deficiencies and should be disseminated only to those individuals with a need to know.

FISMA requires Inspectors General or an independent external auditor, as determined by the Inspector General, to perform an annual independent evaluation of their agency's security program and practices. GSA contracted with KPMG LLP (KPMG), an independent public accounting firm, to conduct this annual evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) *Quality Standards for Inspection and Evaluation* and the Office of Management and Budget's (OMB's) FISMA reporting requirements. This independent evaluation did not constitute an engagement in accordance with the Government Accountability Office's *Government Auditing Standards.*

The objective for this independent evaluation was to assess the effectiveness of GSA's information security program and practices for the period October 1, 2019, through September 30, 2020, for its information systems, including GSA's compliance with FISMA and related information security policies, procedures, standards, and guidelines.

We monitored KPMG's work and reviewed their report and related documentation to ensure professional standards and contractual requirements were met. Our review was not intended to enable us to express, and we do not express, opinions on the effectiveness of GSA's information security controls or on whether GSA's security program complied with FISMA. KPMG is responsible for the attached report and the conclusions expressed in the report.

However, our review disclosed no instances where KPMG did not comply, in all material respects, with CIGIE's *Quality Standards for Inspection and Evaluation* and OMB's FISMA reporting requirements.

A draft report was provided to the GSA Office of the Chief Information Officer for review and comment. The Office of the Chief Information Officer's response to the draft report is included in its entirety in the attached final report.

The Fiscal Year 2021 independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions.

We appreciate the courtesies and cooperation extended to KPMG and our audit staff by GSA during the evaluation. If you have any questions, please contact R. Nicholas Goco, Assistant Inspector General for Auditing, at (202) 501-2322.

Attachment

**KPMG LLP**
8350 Broad Street Suite 900
McLean, VA 22102

Carolyn Presley-Doss
Deputy Assistant Inspector General for Audit Policy and Oversight
General Services Administration
Office of Inspector General
1800 F St., NW, Suite 5037
Washington, DC 20405

December 1, 2020

Dear Ms. Presley-Doss,

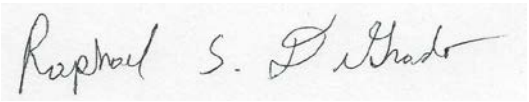
As a deliverable for the FY 2020 General Services Administration (GSA) Office of Inspector General (OIG) Federal Information Security Modernization Act (FISMA) evaluation, we have submitted the *Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2020*. This report is provided to you in the format according to our contract GS-00F-275CA, task order number GSH1416AA0136 and is subject in all respects to the contract terms, including restrictions on disclosure of this deliverable to third parties.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation and in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA), that require us to report our findings and recommendations.

Detailed within the FY 2020 FISMA Report are recommendations to address specific GSA and system-level deficiencies within GSA's information security program and practices. When developing plans of actions and milestones (POA&Ms) or corrective actions, management should assess whether these deficiencies are contained to their respective areas as described in this report or whether the recommendations should be considered for other systems, security control areas, or processes within GSA's information system security program.

Please let me know if you have any questions.

Kind regards,



Raphael DiGrado

# Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2020

November 18, 2020

KPMG LLP
8350 Broad Street, Suite 900
McLean, VA 22102

# U.S. General Services Administration
# Federal Information Security Modernization Act of 2014 Evaluation

## Table of Contents

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

Administrator and Inspector General
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

**Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2020**

This report presents the results of our independent evaluation of the U.S. General Services Administration's (GSA) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including GSA, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2020 FISMA Reporting Metrics to collect these responses. FISMA requires the agency's Inspector General (IG) or an independent external auditor to perform the independent evaluation as determined by the IG. GSA contracted KPMG LLP (KPMG) to conduct this independent evaluation. The Office of Inspector General (OIG) monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

The objective for this independent evaluation was to assess the effectiveness of GSA's information security program and practices for the period of October 1, 2019, to September 30, 2020 for its information systems, including GSA's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work on a selection of GSA-wide security controls and a selection of system-specific security controls across five selected GSA information systems and five GSA contractor-owned information systems[1]. Additional details regarding our independent evaluation scope are included in Appendix I, *Objective, Scope, and Methodology*. Appendix II, *Status of Prior-Year Findings*, summarizes GSA's progress in addressing prior-year recommendations. Appendix III contains a *Glossary* of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, GSA established and maintained its

[1] GSA operates GSA information systems internally, whereas a contractor on behalf of the agency operates contractor systems.

information security program and practices for its information systems for the five cybersecurity functions[2] and eight FISMA metric domains[3]. We assessed the majority of FISMA metric questions as Managed and Measurable (Level 4). Based on the responses we populated into CyberScope[4], we determined that GSA's overall information security program was effective[5] according to DHS guidance. We determined the Detect cybersecurity function to be Optimized (Level 5); the Identify, Protect, and Respond functions to be Managed and Measurable (Level 4); and the Recover function to be Consistently Implemented (Level 3).

While performing FY 2020 entity-wide and information systems' control testing, we identified seven control deficiencies in the Protect Cybersecurity Function within two of the FISMA metric domains – Configuration Management and Identity and Access Management as follows:

Cybersecurity Function/Domain: Protect/Configuration Management

- Unsupported software
- Unauthorized application changes
- Lack of baseline configuration scan review documentation

Cybersecurity Function/Domain: Protect/Identity and Access Management

- Accounts not reauthorized
- Inconsistent documenting of audit alerts
- User accounts not removed timely
- User accounts not authorized

We provided 11 recommendations related to these control deficiencies that should strengthen the respective information systems and GSA's information security program if effectively addressed by management. GSA should also implement a process that ensures similar control deficiencies are addressed across all information systems. In a written response, the GSA Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response, page 17*).

[2] OMB, DHS, and CIGIE developed the FY 2020 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2020, the eight IG FISMA metric domains were aligned with the five cybersecurity functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[3] As described in the DHS' *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0, April 17, 2020,* the eight FISMA metric domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

[4] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology (IT) security reporting for federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, OIGs provide an independent assessment of the effectiveness of an agency's information security program. The Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

[5] The scoring methodology is described in the DHS' *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0 April 17, 2020,* which requires a Managed and Measurable rating (Level 4) to be considered effective as computed by the entries in CyberScope.

This independent evaluation did not constitute an engagement in accordance with *Generally Accepted Government Auditing Standards.* KPMG did not render an opinion on GSA's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting our evaluation results to future periods or other GSA information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

November 18, 2020

# BACKGROUND

## *Federal Information Security Modernization Act*

Title III of the E-Government Act of 2002 (the Act), which was amended in 2014 and commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for information and information systems supporting the agency's operations and assets, including those provided or managed by another agency, contractor, or other source. The Act assigns specific responsibilities to agency heads and IGs in complying with requirements of FISMA. The Act is supported by OMB, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies and procedures. OMB has delegated some responsibility to DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the DHS*, for the operational aspects of federal cybersecurity, such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

### *FY 2020 Inspector General FISMA Reporting Metrics*

For FY 2020, OMB, DHS, and CIGIE updated the IG FISMA reporting metrics to reflect changes to laws and guidance for the five cybersecurity functions and the eight FISMA metric domains. The IG FISMA questions are still organized around the five information security functions[6] outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)[7] and the eight FISMA metric domains[8]. **Table 1** shows the alignment of the Cybersecurity Framework to the FISMA Metric Domains.

| Cybersecurity Framework Security Functions | FY 2020 IG FISMA Metric Domains |
|---|---|
| Identify | Risk Management |
| Protect | Configuration Management<br>Identity and Access Management<br>Data Protection and Privacy<br>Security Training |
| Detect | Information Security Continuous Monitoring |
| Respond | Incident Response |
| Recover | Contingency Planning |

**Table 1:** Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2020 IG FISMA Metric Domains.

[6] In its Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST created Functions to organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[7] The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between the government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

[8] As described in the DHS' *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0, April 17, 2020,* the eight FISMA metric domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

## OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, GSA established and maintained its information security program and practices for its information systems for the five cybersecurity functions and eight FISMA metric domains. Based on the responses we populated into CyberScope, we determined that GSA's overall information security program was effective according to DHS guidance because the majority of the FISMA metric questions were Managed and Measurable (Level 4). We determined the Detect cybersecurity function to be Optimized (Level 5); the Identify, Protect, and Respond functions to be Managed and Measurable (Level 4); and the Recover function to be Consistently Implemented (Level 3). The *Findings* section of this report presents the 7 deficiencies and 11 recommendations. The status of these findings will be assessed as part of the FY 2021 independent evaluation.

Additionally, we evaluated the prior-year findings from the FYs 2019, 2018, 2017, and 2016 FISMA evaluations and determined that GSA had closed six of eight findings. See Appendix II, *Status of Prior-Year Findings*, for additional details.

In a written response to this report, the GSA CIO agreed with our findings and recommendations (see *Management Response, page 17*).

**FINDINGS**

## 1. Protect Function – Configuration Management – Unsupported Software

We determined that as of December 2018, the vendor no longer supports the database version that was in production and supporting a system. GSA implemented a current version of the database on August 20, 2020.

GSA Information Technology (IT) Security Procedural Guide: Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30 Revision 17, July 1, 2020, Section 8 Additional NIST Controls Required by GSA, pages 48-49, states:

> GSA requires certain controls be a part of a systems control set, regardless of a system's specific [Authorization and Accreditation] A&A process, in accordance with the applicability listed in the following table.

| Control No. | Control Name/Statement | Control Applicability |
|---|---|---|
| SA-22 | **Unsupported System Components**<br>The organization:<br>a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and<br>b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs. | • All Systems |

GSA informed us that the vulnerability scans performed by the cloud service provider, who was responsible for this service, did not have the appropriate plugins enabled to identify that the vendor no longer supported the database version used by the application. The information system program team was not checking the vendor's website for the availability of patches, which is a best practice recommended by the Cybersecurity and Infrastructure Security Agency (CISA). Without having a current and supported software running on systems, the risk that security vulnerabilities could be exploited increases, therefore increasing the risk that the confidentiality, integrity, and availability of the data residing on the information system is compromised.

**RECOMMENDATIONS:**

1. Implement a monitoring process to track and identify software components that are no longer supported by vendors and update to a currently supported version, as appropriate.
2. For platform as a service providers, implement a monitoring process that verifies that vulnerability scans, which are provided to GSA, are configured to identify outdated software, which is the responsibility of GSA to update.

## 2. Protect Function – Configuration Management – Unauthorized Application Changes

We determined that five out of five selected application changes did not have authorization prior to implementation into the production environment for one information system selected for testing.

GSA Information Technology (IT) Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, Revision 4, January 17, 2018, Section 4.3 CM-3 Configuration Change Control, page 11, states:

> Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. This control focuses on defining the CM process, controlling the information system configuration according to that process, and ensuring that no configuration changes are made without going through the approved change control process. Below are some general guidelines which can be included in the CM Plan template available on GSA InSite.
>
> - Manage configuration changes to the information system through a chartered Configuration Control Board (CCB) that approves proposed changes to the system. The CCB should monitor the following:
>   - Changes to the information system, including upgrades, modifications, and maintenance changes
>   - Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers).
>   - Emergency changes
>   - Changes to remediate flaws.
> - Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process.
> - Conduct a security impact analysis (per CM-4) to determine the ramifications of the proposed change. Consider changes only after analyzing the results of the security impact analysis.
> - Use automated tools/processes to control/manage system changes. If automated tools are not used, a GSA Change Request Form (Appendix A) is provided.
> - Document all approved configuration-controlled changes in appropriate documentation. The current state of the system should be the 'as-built' configuration as reflected in the initial baseline with approved changes.
> - Audit activities associated with configuration changes to the information system.
> - Review the approved configuration management process for key auditable activities and then review records of selected activities in the process; for example:
>   - Who approved the change request;
>   - Who implemented the change;
>   - Who completed the security impact assessment;
>   - Who tested the change; and
>   - How it was tested.
> - Ensure that any testing performed does not adversely impact the information system (perform the test on a test platform, not a production platform).

GSA did not follow the documented process of obtaining authorizations for the application changes. Without implementing effective configuration management controls, the risk increases that unauthorized access could be permitted to introduce fraudulent data or malicious code into

the application without detection. This also increases the risk that the confidentiality, integrity, and availability of the data residing on the information system could be compromised.

**RECOMMENDATIONS:**

1. Design and implement a quality control process to validate that designated agency officials have authorized all application changes prior to implementing these changes in the production environment.
2. Evaluate and document the five unauthorized changes to confirm that the system's production environment was not adversely affected.

## 3. Protect Function – Configuration Management – Lack of Baseline Configuration Scan Review Documentation

We determined that for one out of five selections for one information system selected for testing, evidence of management's baseline configuration scan review was not available.

GSA Information Technology (IT) Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, Revision 4, January 17, 2018, Section 4.6. CM-6 Configuration Settings, pages 14-15, states:

> Configure systems in agreement with GSA technical guidelines/benchmarks. GSA benchmarks may be exceeded but not lowered. If no technical guideline/benchmark is available for a particular technology, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines may be used, as deemed appropriate by the [Authorizing Official] AO. Configure the security settings to the most restrictive mode consistent with operational requirements in all components of the information system.
>
> Security settings that are not completely implemented because of operational requirements should be documented in the [System Security Plan] SSP. Any deviations, not following GSA policies and standards must be submitted using the Security Deviation Request Google Form. The system owner must monitor and control changes in accordance with the CM Plan and GSA policies and procedures. GSA's [Security Operations (SecOps)] ISO Division scans for configuration compliance on a regular basis and provides the data to the appropriate system POC for resolution.
>
> For enhancements CM-6(1) and (2), GSA uses automated tools that are installed and integrated into GSA's Enterprise Logging Platform to verify configuration settings and alert personnel to respond to unauthorized changes.

GSA asserted that they did not retain supporting documentation of the baseline configuration scan review due to turnover at the ISSO position. Therefore, management could not provide evidence of baseline configuration scan review for one out of five scan reports due to the transition of the ISSO position. Without maintaining evidence of baseline configuration scan reviews, the potential exists that system security officials are unaware of security configuration weaknesses or vulnerabilities that could compromise the operation and integrity of the system.

**RECOMMENDATION:**

1. Implement a consistent method to document and retain management's review of system baseline configuration scans that includes the actions performed, who performed the review, and the date of the review.

## 4. Protect Function – Identity and Access Management – Accounts Not Reauthorized

We determined individuals who have privileged access for infrastructure accounts (operating system and database) perform a self-reauthorization.

GSA Information Technology (IT) Security Policy Chief Information Officer (CIO) 2100.1L:

> Chapter 2: Security Roles and Responsibilities, Section 12. System Owners, page 20, states:
> k. Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).
>
> Chapter 4: Policy for Protect Function, Section 1 Identity management, authentication and access control, page 37, states:
> d. Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all user accounts shall be completed annually to ensure the continued need for system access.

GSA currently does not require supervisors to perform reauthorization of privileged access for users that report to them. Without implementing an effective reauthorization process where the system owner or supervisor performs the validation that the individual still has a business need for the privileged access, excessive privileges could be permitted.

**RECOMMENDATIONS:**

1. Implement the new controls that restrict privileged operating system and database users from self-reauthorizing their accounts.
2. Update GSA Security policies to require privileged operating system and database user accounts to be reauthorized on a more frequent basis.

**5. Protect Function – Identity and Access Management – Inconsistent Documenting of Audit Alerts**

We determined that management, for three information systems selected for testing, was not consistently documenting its review of the audit log alerts for each system.

GSA Information Technology (IT) Security Policy Chief Information Officer (CIO) 2100.1L, Chapter 5: Policy for Detect Function, Section 2. Security continuous monitoring, page 62, states:

> d. Monitoring procedures must include specific steps to be taken and protocol to be applied when reviewing audit/log data.

GSA Information Technology (IT) Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08, Revision 5, November 3, 2017, Section 3.6. AU-6 Audit Review, Analysis, and Reporting, page 14, states:

> System Specific Expectations for GSA/Internally Operated Systems: The system owner maintains the responsibility of reviewing information system logs on their systems for unusual activity on a periodic basis defined on a system by system basis, and should keep a log that such a review has taken place.

The security teams for each system were not following GSA policy that requires a log to be maintained to support actions taken when alerts are received. By not consistently documenting the actions taken when an audit log alert is received as stipulated by GSA security policy, the potential exists that unusual activity may not be investigated appropriately, and critical system data could be compromised.

**RECOMMENDATION:**

1. Implement a consistent method to document the review of audit log alerts that includes the actions performed, who performed the review, the date of the review, and maintain the evidence.

## 6. Protect Function – Identity and Access Management – User Accounts Not Removed Timely

We determined that GSA did not remove user accounts timely for separated individuals from October 1, 2019, through June 30, 2020, for three systems:

- Five out of 721 separated individuals maintained an active network account past the allotted 30 days after separation from the Agency.
- One out of 721 separated GSA individuals maintained an active user account past the allotted 30 days after separation from the Agency, for one information system selected for testing.
- Two out of 721 separated GSA individuals maintained active user accounts past the allotted 30 days after separation from the Agency, for one other information system selected for testing.

All separated individuals' user accounts, cited above, have subsequently been removed.

GSA Information Technology (IT) Security Policy Chief Information Officer (CIO) 2100.1L, Chapter 4: Policy for Protect Function, Section 1. Identity management, authentication and access control, page 37, states:

> e. Disabling and removal of user accounts supporting account management processes, to include:
>
> (1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.
>
> (2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the [Office of the Chief Information Security Officer] OCISO (e.g., separation lists, role revisions). Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

GSA Information Technology (IT) Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 4, June 4, 2019, Section 6.1. PS-4 Personnel Termination, page 11-12, states:

> Control: The organization, upon termination of individual employment:
> a. Disables information system access within [*24 hours after an approved Service Catalog Request indicating personnel termination*]

For the netowork accounts, the account removal tickets were not submitted by the users' supervisors when the users left GSA. For one information system user account, an account removal ticket was submitted to remove the network account, but the account removal ticket did not include the removal of their application administrator account. For one information system, management was not following GSA policy that requires the users' supervisors to submit an account removal tickets in order to remove information system access.

Without removing separated users' access from information systems within 30 days of separation from GSA, the potential exists for an unauthorized user to gain access to the system. This could result in unnecessary system downtime and modification, destruction, or exposure of critical data.

**RECOMMENDATIONS:**

1. Disable/remove the separated users' accounts.
2. Implement a monitoring control to perform a comparison of the separations listing, ticketing system deletes, and active user accounts on a monthly basis to identify and remove user accounts that were missed during the normal exiting/off-boarding process.

## 7. Protect Function – Identity and Access Management – User Accounts Not Authorized

We determined the following:

- For one information system selected for testing, management did not formally authorize one out of one new user account selected for testing before the account was created in the system.
- For one other information system selected for testing, management did not formally authorize one out of seven new user accounts selected for testing before the account was created in the system.

GSA Information Technology (IT) Security Policy Chief Information Officer (CIO) 2100.1L, Chapter 4: Policy for Protect Function, Section 1 Identity management, authentication and access control, page 37, states:

> f. Request, including modifications, and approval routing in support of account management processes must ensure:
> (1) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;
> (2) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the data or system owner;
> (3) Access requests are routed to the data or system owner by a user's supervisor, COR, ISSO, ISSM, director, or designated official.

GSA Information Technology (IT) Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07, Revision 4, May 8, 2017, Appendix B: GSA CIO Order 2100.1 Policy Statements on Access Control Chapter 5, Page 37, states:

> e. Account Management (Chapter 5, Paragraph l)
> (1) Request and approval routing in support of account management processes must assure:
> (a) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;
> (b) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the Data or System Owner;
> (c) Access requests may be aggregated and managed by designated coordinators for efficiency;
> (d) Access requests are routed to the data or System Owner by a user's supervisor, COR, ISSO, ISSM, director, or designated regional coordinator.
>
> (2) Authorizations supporting the account management processes must assure:
> (a) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know;
> (b) Data owners/system owners, with assistance from the designated ISSO, ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual Information Security & Privacy Act training curriculum. System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of

need-to-know. Contractors with system access must utilize a gsa.gov e-mail account to conduct business with GSA.

GSA did not follow the documented process for user account creation. Without obtaining authorizations for new user access, there is an increased risk that unauthorized access could be permitted and therefore increase the risk that the confidentiality, integrity, and availability of the data residing on the information systems could be compromised.

**RECOMMENDATION:**

1. Provide training to individuals responsible for information system user account creation and authorization to emphasize adherence to the access authorization controls described in the respective SSPs and GSA IT Security Procedural Guide: AC CIO-IT Security-01-07.

## MANAGEMENT RESPONSE TO THE REPORT

DocuSign Envelope ID: 6C615F70-80B5-43FF-9EBD-84B99E570929

**GSA IT Office**

11/10/2020

MEMORANDUM FOR CAROLYN PRESLEY-DOSS
DEPUTY ASSISTANT INSPECTOR GENERAL
FOR AUDIT POLICY AND OVERSIGHT – JA

FROM DAVID A. SHIVE
CHIEF INFORMATION OFFICER – I

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Agency Management Response – Discussion Draft
*Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2020*

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation report entitled Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2020. We agree with the findings and recommendations stated in the report.

If you have any questions or concerns, please contact Bo Berlas, Chief Information Security Officer (CISO) of my staff, on 202-236-6304.

**U.S. General Services Administration**
1800 F Street NW Washington,
DC 20405 www.gsa.gov

## APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective for this FISMA evaluation was to conduct an independent evaluation of GSA's information security program and practices to assess the effectiveness of such program and practices for the period of October 1, 2019, to September 30, 2020. The specific objectives of this evaluation were to:

- Perform the annual independent FISMA evaluation of GSA's information security program and practices;
- Respond to the DHS FY 2020 Inspector General FISMA Reporting Metrics; and
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the CIGIE's Quality Standards for Inspection and Evaluation and applicable AICPA standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, presidential directives, and the DHS *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0,* dated April 17, 2020, and NIST standards and guidelines as outlined in the *Criteria* section below. We reviewed GSA's information security program for a program-level perspective and then examined how each of the information systems selected for our testing implemented these policies and procedures.

We selected 10 information systems (5 GSA information systems and 5 contractor-owned information systems) from a total population of 112 major applications and general support systems as of March 2, 2020. We also performed follow-up testing on three GSA information systems and three GSA contractor-owned information systems to determine if GSA had closed the prior-year findings.

Our procedures included the following to assess the effectiveness of the information security program and practices of GSA:

- Inquiry of information system owners, ISSOs, ISSMs, system administrators, and other relevant individuals to walk through each control process;
- An inspection of the information security practices and policies established by the Office of GSA IT;
- An inspection of the information security practices, policies, and procedures in use across GSA; and
- An inspection of artifacts to determine the implementation and operating effectiveness of security controls.

We performed our fieldwork, observations, and inquiries using GSA's collaboration tools during the period of April 20, 2019, through September 30, 2020. During our evaluation, we met regularly with GSA management to provide a status of the engagement and discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications (SPs) provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the FY 2020 FISMA evaluation:

**NIST, Federal Information Processing Standard (FIPS), and/or SPs[9]**

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST Cybersecurity Framework Version 1.1, *Framework for Improving Critical Infrastructure Cybersecurity*
- NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*
- NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST Special Publication 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
- NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-60 Volume 1, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-63-3, *Digital Identity Guidelines*
- NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
- NIST Special Publication 800-184, *Guide for Cybersecurity Event Recovery*
- NIST Supplemental Guidance on Ongoing Authorization, *Transitioning to Near Real-Time Risk Management*

**OMB Policy Directives**

- Federal Enterprise Architecture (FEA) Framework, Version 2

[9] Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Memorandum 08-05, *Implementation of Trusted Internet Connections (TIC)*
- OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum 17-09, *Management of Federal High Value Assets*
- OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB Memorandum 17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- OMB Memorandum 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum 19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum 20-04, *Guidance on Federal Information Security and Privacy Management Requirements*

**United States Department of Homeland Security**

- DHS Binding Operational Directive 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*
- FCD-1, *Federal Continuity Directive 1*
- FCD-2, *Federal Continuity Directive 2*
- FY 2020 Chief Information Officer (CIO) Federal Information Security Modernization Act Metrics, Version 1, October 2019
- FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0, April 17, 2020
- United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines
- US-CERT Federal Incident Reporting Guidelines
- Homeland Security Presidential Directive (HSPD) 12, *Policy for a common Identification Standard for Federal Employees and Contractors*
- DHS Binding Operational Directive 18-02, *Securing High Value Assets*

**GSA Policy and Procedural Guides**

- GSA IT Security Policy CIO 2100.1L, July 15, 2019
- IT Security Procedural Guide: Risk Management Strategy, CIO-IT Security-18-91 Revision 3, June 25, 2020
- IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk, CIO-IT Security-06-30, Revision 17, July 1, 2020
- IT Security Procedural Guide: Information Security Program Plan, CIO-IT Security-18-90, Revision 3, June 16, 2020
- IT Security Procedural Guide: Federal Information Security Modernization Act (FISMA) Implementation, CIO-IT Security-04-26, Revision 2, April 16, 2019
- GSA Order ADM 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing Policy, and Background Investigations for Contractor Employees, March 18, 2020
- IT Security Procedural Guide: Plan of Action and Milestones (POA&M), CIO-IT Security-09-44, Revision 6, April 6, 2020

- GSA Order ADM 2400.1A, Insider Threat Program, May 18, 2016
- IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts, CIO-IT Security-09-48, Revision 4, January 25, 2018
- IT Security Procedural Guide: Configuration Management (CM), CIO-IT Security-01-05, Revision 4, January 17, 2018
- IT Security Procedural Guide: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Implementation Guide, CIO-IT Security-14-69, Revision 4, May 26, 2020
- IT Security Procedural Guide: Identification and Authentication (IA), CIO-IT Security-01-01, Revision 6, March 20, 2019
- IT Security Procedural Guide: Termination and Transfer, CIO-IT Security-03-23, Revision 4, June 4, 2019
- IT Security Procedural Guide: Access Control, CIO-IT Security-01-07, Revision 4, May 8, 2017
- IT Security Procedural Guide: Audit and Accountability (AU), CIO-IT Security-01-08, Revision 5, November 3, 2017
- IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program, CIO-IT Security-05-29, Revision 6, May 1, 2020
- IT Security Procedural Guide: Contingency Planning (CP), CIO-IT Security-06-29, Revision 5, July 27, 2020
- IT Security Procedural Guide: Information Security Continuous Monitoring Strategy (ISCM) & Ongoing Authorization (OA) Program, CIO-IT Security-12-66, Revision 3, April 23, 2020
- IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02, Revision 17, March 20, 2019
- GSA Order CIO P 1878.1, GSA Privacy Act Program, September 2, 2014
- GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII), October 29, 2014
- GSA Order CIO 2100.3C, Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities, June 23, 2016
- GSA Order ADM 2470.2, Occupant Emergency Plan, November 17, 2017
- GSA Order CIO 1878.3, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices, January 23, 2019
- IT Security Procedural Guide: Vulnerability Management Process, CIO-IT Security-17-80, Revision 1, August 21, 2019
- GSA Order CIO 9297.2C CHGE 1, GSA Information Breach Notification Policy, March 27, 2019
- IT Security Procedural Guide: External Information System Monitoring, CIO-IT Security-19-101, Initial Release, October 22, 2019
- GSA Order ADM 9732.1E, Personnel Security and Suitability Program Handbook, March 12, 2019

**Other Directives, Policies, and Legislation**

- National Insider Threat Policy, Presidential Executive Order (EO) 13587, November 21, 2012
- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Presidential EO 13800, May 11, 2017
- Federal Cybersecurity Workforce Assessment Act of 2015, Senate 2007 (S.2007), Public Law 114-113, December 1, 2015
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
- National Archives and Records Administration's (NARA) guidance on information systems security records, General Records Schedule (GRS) 3.2, September 2016
- CFO Council ERM Playbook, *Enterprise Risk Management for the U.S. Federal Government CFO Chief Financial Officers Council*, July 29, 2016

- Federal Acquisition Regulation (FAR) Case 2007-004, *Common Security Configurations*
- Presidential Policy Direction (PPD) 41, *United States Cyber Incident Coordination*
- U.S. Government Accountability Office (GAO) – Standards for Internal Control in the Federal Government, September 10, 2014
- *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, SECURE Technology Act, U.S. House of Representatives 7327 (H.R.7327), December 21, 2018

## APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

As part of this year's FISMA Evaluation, we followed up on the status of open prior-year findings. We evaluated the information systems to determine whether the recommendations have been implemented and closed by management. If there was evidence that the recommendations had been sufficiently implemented, we determined the finding closed. If there was evidence that the recommendations had been only partially implemented or not implemented at all, we determined the finding to be open. Based on our testing, we determined six of eight prior year findings were closed.

**Prior Year Findings – Evaluation**

**Prior Year Findings – 2016 Evaluation**

| Finding Number | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **4. Identity and Access Management – Account Management** | We identified a terminated application user maintained access to the system past the allotted 30 days from separation. | 3. Remove terminated users from systems within the required timeframe. | 3. Closed |

**Prior Year Findings – 2017 Evaluation**

| Finding Number | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **1. Identify Function – Risk Management**<br><br>**Contractor Systems** | We determined that GSA was receiving the required contractor deliverables for five contractor systems. However, we noted instances where the review and acceptance of the deliverables was not documented, did not follow a formal process when comments or concerns were presented to the contractor, and did not obtain sufficient assurance that GSA was monitoring the performance of the services provided by the contractor. | 1. Implement a formalized review and acceptance process of contractor deliverables that includes the information system security officer ISSO and ISSM review of the information, and COR acceptance of the deliverable. | 1. Closed |
| **2. Protect Function – Configuration Management**<br><br>**Change/Patch Management Approval** | We identified a system authorization and testing evidence for Quarter 1 and Quarter 3 application changes and the November 2016 Linux and Windows operating system patches could not be provided. | 2. Document evidence of authorization of application changes, and operating system and database patches.<br><br>Updated recommendation:<br>Document evidence of testing and authorization of operating system patches. | 2. Closed |
| **3. Protect Function – Identity and Access Management**<br><br>**Account Management** | We identified privileged account reviews for the operating system and database for a system were not performed in accordance with GSA policy to verify that the individuals needed privileged access. | 1. Implement a formal process for approving, reviewing, and removing privileged access for the system. | 1. Closed |

**Prior Year Findings – 2018 Evaluation**

| Finding Number | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **3. Protect Function – Identity and Access Management**<br><br>**Account Management** | We identified the following exceptions:<br>1. For one out of 634 separated users, GSA did not remove access to the user's network account timely (within 30 days of user separation). | We recommend GSA perform the following actions:<br>2. Compare the Separations Report to the Active Directory user listing on a monthly basis to ensure separated users are removed from the Active Directory. | 2. Open – See Finding 6 in the current year section of the report. |

**Prior Year Findings – 2019 Evaluation**

| Finding Number | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **1. Identify Function – Risk Management**<br><br>**Contractor Systems** | We determined for both contractor information systems selected for testing that there was only partial or no evidence for certain required deliverables used to monitor contractors' compliance with GSA security requirements that the Contracting Officer's Representative (COR), Information System Security Officer (ISSO), and Information System Security Manager (ISSM) reviewed and accepted. | 1. Implement a standard, formal contractor deliverable review and acceptance process by the COR that includes a review by the ISSO/ISSM. | 1. Closed |
| **2. Protect Function – Identity and Access Management**<br><br>**Account Management** | We determined that 1 out of 613 separated GSA employees from October 1, 2018 through June 30, 2019 maintained an active network account past the allotted 30 days from separation. | 1. We recommend that GSA implement a monitoring control to review rejected tickets related to separated employees and contractors on a monthly basis. | 1. Open – See Finding 6 in the current year section of the report. |

| Finding Number | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **3. Respond Function – Incident Response**<br><br>**Incident Response** | Out of a population of 48 incidents reportable to US-CERT, we selected 11 incidents for testing and we determined that GSA IT did not report 2 out of the 11 incidents to US-CERT within the one hour timeframe. | We recommend GSA:<br>1. Implement a monitoring control to ensure incidents are reported timely to US-CERT.<br>2. Provide training to new analysts on the GSA incident reporting process, including how to submit incidents to US-CERT. | 1. Closed<br><br>2. Closed |

## APPENDIX III – GLOSSARY

| ACRONYM | DEFINITION |
|---|---|
| A&A | Authorization and Accreditation |
| AC | Access Control |
| AICPA | American Institute of Certified Public Accountants |
| AO | Authorizing Official |
| AU | Audit and Accountability |
| CCB | Change Control Board |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| CIO | Chief Information Officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CM | Configuration Management |
| COR | Contracting Officer's Representative |
| CP | Contingency Planning |
| CSIP | Cybersecurity Strategy and Implementation Plan |
| DHS | Department of Homeland Security |
| EO | Executive Order |
| FAR | Federal Acquisition Regulation |
| FEA | Federal Enterprise Architecture |
| FICAM | Federated Identity, Credential, and Access Management |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GAO | U.S. Government Accountability Office |
| GRS | General Records Schedule |
| GSA | U.S. General Services Administration |
| HSPD | Homeland Security Presidential Directive |
| IA | Identification and Authentication |
| IG | Inspector General |
| IR | Incident Response |
| ISCM | Information Security Continuous Monitoring |
| ISO | Security Operations |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| KPMG | KPMG LLP |
| NARA | National Archives and Records Administration |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| OA | Ongoing Authorization |

| ACRONYM | DEFINITION |
|---|---|
| OCISO | Office of Chief Information Security Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| POA&M | Plan of Action and Milestones |
| PPD | Presidential Policy Direction |
| SP | Special Publication |
| SSL | Secure Sockets Layer |
| SSP | System Security Plan |
| The Act | Title III of the E-Government Act of 2002 |
| TIC | Trusted Internet Connections |
| TLS | Transport Layer Security |
| US-CERT | United States Computer Emergency Readiness Team |